

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problems Mailbox.**

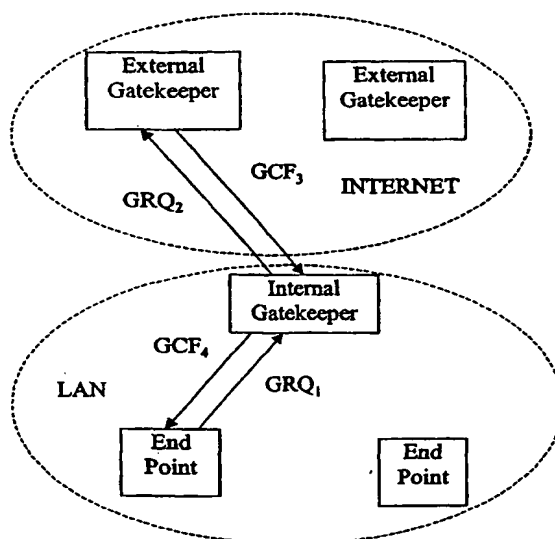
**THIS PAGE BLANK (USPTO)**



## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification <sup>7</sup> : <b>H04L 12/66</b>		A1	(11) International Publication Number: <b>WO 00/48368</b>
			(43) International Publication Date: 17 August 2000 (17.08.00)
(21) International Application Number: PCT/NO00/00030		(81) Designated States: AE, AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), DM, EE, EE (Utility model), ES, FI, FI (Utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KR (Utility model), KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).	
(22) International Filing Date: 2 February 2000 (02.02.00)			
(30) Priority Data: 19990593 9 February 1999 (09.02.99) NO 09/387,355 31 August 1999 (31.08.99) US			
(71) Applicant (for all designated States except US): TELEFONAKTIEBOLAGET LM ERICSSON [SE/SE]; S-126 25 Stockholm (SE).			
(72) Inventors; and			
(75) Inventors/Applicants (for US only): CORNELIUSSEN, Knut, Snorre, Bach [NO/NO]; Bygdøy allé 117A, N-0273 Oslo (NO). KLILAND, Kevin [NO/NO]; Finstadsvingen 11, N-1400 Ski (NO). IVELAND, Espen [NO/NO]; Rings gate 6, N-3045 Drammen (NO). SKJÆRAN, Espen [NO/NO]; Guldbergs vei 27, N-0375 Oslo (NO).			
(74) Agent: OSLO PATENTKONTOR AS; Postboks 7007 M, N-0306 Oslo (NO).		<p><b>Published</b></p> <p>With international search report.</p> <p>Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</p>	

(54) Title: AN ARRANGEMENT FOR DISTRIBUTING AND DESPATCHING TRAFFIC IN A NETWORK, ESPECIALLY H.323 GENERATED TRAFFIC



## (57) Abstract

The present invention relates to an arrangement for distributing and dispatching traffic in a network, especially H.323 generated traffic, which arrangement comprises one or more gatekeepers, here designated as so-called external or real gatekeepers, and for the purpose of utilising such real gatekeepers in a far more efficient and cost saving manner, and also for avoiding reconfiguration of endpoints depending on which gatekeepers with which they want to communicate, the present invention suggests a solution characterized by the introduction of one or more internal gatekeepers, here also designated as so-called internal lightweight gatekeepers, each such internal gatekeeper basically understanding any message used by any endpoint when registering to a real gatekeeper.

**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

**AN ARRANGEMENT FOR DISTRIBUTING AND DESPATCHING TRAFFIC IN  
A NETWORK, ESPECIALLY H.323 GENERATED TRAFFIC**

Field of the invention

5

The present invention relates to an arrangement for distributing and dispatching traffic in a network, especially H.323 generated traffic, which arrangement comprises one or more gatekeepers, here designated as so-called external or  
10 real gatekeepers.

The problem areas

Today there does not exist any lightweight solution for distributing and dispatching H.323 generated traffic.

15

Known solutions and problems with these

It is perfectly possible to distribute and dispatch H.323 by using a gatekeeper. It might however be costly to run a full fledged gatekeeper for distributing and dispatching  
20 H.323 generated traffic if the intention only is to distribute and dispatch H.323 generated traffic. A real gatekeeper is complex and has to know about lots of messages etc. described in H.323. An endpoint may be any kind of H.323 based equipment.

25 In H.323 version 2, redundancy of gatekeepers are described, where one gatekeeper is instructing the endpoint to contact another known gatekeeper if itself can not fulfil the service requested. It requires however that end-

points understand version 2 of the protocol, and interpret the message fields. This solution is not applicable for load balancing, as it has no mechanism for one real gatekeeper to know of the other, or any mechanism to report  
5 load between them.

### Objects of the invention

An object of the present invention is to provide an arrangement by which the distribution and dispatch of H.323  
10 generated traffic can be provided in a far more expedient and less costly manner.

Another object of the present invention is to provide an  
15 arrangement by which endpoints can be put in contact with so-called external or real gatekeepers without having to be reconfigured depending on which gatekeeper they want to communicate with.

20 A further object of the present invention is to provide an arrangement by which supplementary achievements, comprising for example load balancing, QoS (Quality of Service), information about cost, etc. can easily be implemented.

25 Still another object of the present invention is to provide an arrangement by which the messages associated with so-called external or real gatekeepers are utilised in a rational and effective manner.

Brief disclosure of the invention

The above objects are achieved in an arrangement as stated in the preamble, which according to the present invention is characterized by the introduction of one or more internal and lightweight gatekeepers, where internal means that they are arranged in a certain domain, and they are lightweight in the sense that each gatekeeper support a limited range of the H.323 message set, each such lightweight gatekeeper basically understanding any message used by any endpoint when registering to a real gatekeeper and that each lightweight gatekeeper is adapted to put an endpoint of its domain in contact with an external or real gatekeeper, outside said domain.

In other words, the present invention performs the H.323 distribution and dispatch by utilising an extreme lightweight gatekeeper that basically understands the GRQ (Gatekeeper Request), GCF (Gatekeeper Confirm) and GRJ (Gatekeeper Reject) H.323 RAS messages.

These messages are stated in H.225 and are used by endpoints when registering to a gatekeeper. Such a lightweight gatekeeper is able to put an endpoint within the lightweight gatekeeper's domain in contact with a full fledged or real gatekeeper outside its own domain.

How to achieve supplementary achievements as e.g. load balancing is also described in the text below. Some of the ways described here not only involves GRQ, GCF and GRJ.

Further features and advantages of the present invention will appear from the following description taken in conjunction with the enclosed drawings.

5 Brief description of the drawings

Figure 1 is a sketch of a typical scenario in which the distributed gatekeeper system might be utilised with endpoints, internal (lightweight) gatekeeper located inside  
10 the domain or LAN and external (real) Gatekeepers located outside. The network components as e.g. routers etc. are not outlined.

Figure 2 is a network scenario in which the distributed  
15 gatekeeper system may be applied. Not all of the components within the ISP domain are outlined, neither is network-related equipment as e.g. routers etc. outlined. An example of a LAN domain is sketched in Figure 1. The internal gatekeepers may be connected in any way and any number towards  
20 the external gatekeepers. An arbitrary number of external gatekeepers may be connected.

Figure 3 shows the message exchange during start up of a real gatekeeper, when the real gatekeeper register a light-  
25 weight gatekeeper.

Figure 4 shows the message transfer in communication between real and lightweight gatekeeper, as the lightweight gatekeeper collects information relating to e.g. the load  
30 situation of the real gatekeeper.

Figure 5 gives a system overview.



Detailed description of embodiments

An endpoint that wants to initiate a session towards another endpoint has first to register to a gatekeeper. An endpoint performs this by sending a GRQ (see Figure 1 GRQ<sub>1</sub>) to the lightweight gatekeeper. The lightweight gatekeeper only understands and responds to GRQs. As the lightweight gatekeeper also has knowledge of real gatekeepers outside its own domain, it responds to the endpoint with a GCF (see Figure 1 GRQ<sub>4</sub>) with the gatekeeper id of an appropriate full fledged gatekeeper outside its own domain. In advance the lightweight gatekeeper must have gained knowledge of valid gatekeepers outside its domain (information like IP address). The method for gaining and updating the knowledge of external gatekeepers is described in the text below, in connection with the discussion of Figure 4. In addition, each time an endpoint connects to the lightweight gatekeeper, the lightweight gatekeeper should use the same signals, i.e. GRQ (see Figure 1 GRQ<sub>2</sub>) and GCF (see Figure 1 GRQ<sub>3</sub>), towards the real gatekeepers e.g. to check which gatekeepers that allow the endpoint to be connected.

Figure 1 only indicates one possible scenario on how the lightweight gatekeeper communicates with the real gatekeepers. Alternatively the internal gatekeeper may directly provide the address of an external gatekeeper in the GCF towards the endpoint as a response to the GRQ. Figure 2 indicates how the arrangement is deployed when taking ISPs, LAN and Internet into account.

Load balancing may be obtained through the inventive method. The lightweight gatekeeper has knowledge of valid real gatekeepers' load and, on this basis, the lightweight gatekeeper might distribute the traffic towards the least loaded gatekeeper.

Each real gatekeeper should be configured to know a lightweight gatekeeper, and should register with this during start-up. This can be done using Registration Request (RRQ). The lightweight gatekeeper replies with Registration Confirm (RCF) including an endpoint identifier, which the real gatekeepers may use in future communication with the lightweight gatekeeper, and adds the real gatekeeper to its internal list of gatekeepers. See Figure 3.

The ResourceAvailabilityIndication (RAI) and ResourceAvailabilityConfirm (RAC) messages (RAS protocol, [1]), are described for use between gateways and gatekeepers. The gateway sends the indication, either periodically, or when the resource situation has changed, to the gatekeeper, which uses this information when picking the gateway a given call is routed to.

This invention utilizes this mechanism between a real gatekeeper and the extended lightweight gatekeeper, in order for the lightweight gatekeeper to make more intelligent choices when forwarding the GRQ message to the gatekeeper that will actually be used for registration and call routing.

A real gatekeeper sends RAI with the endpoint identifier received during registration and its resource situation (see figure 4). The list of gatekeepers in the lightweight gatekeeper will now be updated with resource information so that the gatekeeper dispatcher will not forward a GRQ to a gatekeeper which has indicated that it is almost out of resources.

As an alternative to using RAI/RAC, the proprietary non-StandardData field of GCF and GRJ might be used for exchanging e.g. QoS information between the lightweight gatekeeper and the real gatekeepers. If the lightweight gatekeeper keeps track of each real gatekeeper's e.g. QoS, e.g. in a table form, these tables may be updated each time the lightweight gatekeeper receives a GCF or GRJ from a real gatekeeper. The lightweight gatekeeper will then read the nonStandardData field of these messages and update its tables. In the same way the clients may indicate their willingness to pay and hence achieve corresponding e.g. QoS by using the nonStandardData field of the GRQ message.

*A simple example of how to utilise the nonStandardData field:* E.g. load information might be exchanged between a real gatekeeper and the lightweight gatekeeper by stating that the first byte of the nonStandardData field in the GCF message shall contain an integer indicating the gatekeeper's load. The same idea applies for exchanging other kind of data.

Other ways of exchanging information not involving the nonStandardData field of GCF, GRJ and GRQ are described below.

The lightweight gatekeeper should also be able to handle registration requests (RRQ) from endpoints, but should always reject them (RRJ) with reason discovery required, to enforce endpoints with manual discovery (configured gatekeeper address) to send GRQ.

As this solution is done transparent to the endpoint, it is not required to support version 2 of H.323, or to interpret all the parameters in the messages.

The situation between endpoints, lightweight gatekeeper and real gatekeepers are shown in Figure 5. As the lightweight gatekeeper holds very little cached information (the registrations) there is no need for redundancy for this entity, and it may restart automatically after an unexpected crash. By using a "time to live" parameter in the real-lightweight registrations, the real gatekeepers will automatically re-register at a given interval, and the system is up again. No calls are lost during this period.

Transfer of registered endpoints from one gatekeeper to another, e.g. during shutdown of one gatekeeper for software upgrade, may be done by first unregistering the gatekeeper from the lightweight gatekeeper, and then unregister all registered endpoints. Normally, an endpoint then tries to re-register. This attempt should be rejected with reason discovery required, thereby forcing the endpoint to send GRQ to the lightweight gatekeeper. In this way, gatekeeper redundancy is also achieved for version 1 endpoints, which can not understand the required version 2 fields for gatekeeper redundancy.

Network resource management will be simplified since one node (the lightweight gatekeeper) now knows the resource situation of all the gatekeepers "belonging" to it.

QoS might also be obtained through the approach according to the present invention. If the lightweight gatekeeper is able to and has obtained knowledge of which level of QoS the different gatekeeper providers are able to provide, this information might be utilised for connecting the endpoints to the gatekeeper with the QoS level in mind. An endpoint might not always want to connect to the gatekeeper providing the best QoS because higher QoS might mean higher charge.

Information of the (current) cost of using the different full fledged gatekeepers might also be provided by the same approach as described for load balancing and QoS.

5 Information flow between the lightweight gatekeeper and the real gatekeepers

Several alternatives exist regarding how often the lightweight gatekeeper ought to communicate with the external gatekeepers and hence update the internal tables:

- 1) The lightweight gatekeeper may update its internal tables statically, i.e. by management. An example of a static configuration setting may be that between 0800 and 1000 a certain external gatekeeper doesn't want to handle GRQs coming from the lightweight gatekeeper.
  - 2) The lightweight gatekeeper may update its internal tables partly dynamically, i.e. e.g. on GCF, GRJ and RAI received from the real gatekeepers.
  - 3) Other H.225 or H.245 messages might be utilised for such information exchange, e.g. the H.225's IRQ (InfoRequest) and IRR (InfoResponse)
  - 4) Other ways of exchanging such information also exist. Examples may be to use other protocols like TCP, UDP or such as Java/RMI, CORBA etc.
- Any combination of the above mentioned approaches may be applied. Besides, information on a client's willingness to

pay might be forwarded in the GRQ message, see next chapter.

5 Information flow between endpoints and the lightweight gatekeeper

Information that might flow from endpoints to the lightweight gatekeeper is e.g. willingness to pay information. Hence the lightweight gatekeeper, dependent of the frequency, has valid knowledge of the endpoints, e.g. willingness to pay.

The way in which this information might be exchanged is according to those mechanism described in previous chapter.

15

Which real gatekeeper to put an endpoint in touch with

Another issue is which real gatekeeper the lightweight gatekeeper should put an endpoint in contact with. Alternatives may be:

20

1) Forward the GRQ to a randomly picked real gatekeeper

2) Forward the GRQ based on internal information. Examples of internal information might be QoS, load, cost, time of day etc.

25

3) Forward the GRQ to a specific real gatekeeper on the basis of other criterias

30

4) By forward is meant explicitly, i.e. plain forward of the GRQ to an external gatekeeper, or implicitly, i.e.

the address of the external gatekeeper is directly provided in the internal gatekeeper's GCF towards the endpoint

5 Advantages

Such an extremely lightweight gatekeeper is trivial to implement and only needs small amount of memory and CPU power. Due to these modestly demanding requirements it does  
10 not have to execute on dedicated hardware (PCs, workstations etc.) An advantage that is a consequence of the lightweight approach, is that e.g. a small company that thinks it is too costly to put up an own local gatekeeper might initiate contracts with one or several gatekeeper  
15 providers.

Such a distributed approach is trivial to maintain due to the fact that all the endpoints only needs to know about one gatekeeper, i.e. the lightweight gatekeeper. If the  
20 endpoints communicate directly with the real gatekeepers, the endpoints have to be reconfigured depending on which gatekeepers they want to communicate with.

This invention has the great advantage that it allows a system of multiple gatekeepers to distribute load evenly,  
25 thereby reducing call setup time and improving the total possible utilization compared to the statical endpoint-gatekeeper relationship.

Further the gatekeepers are able to recover automatically after a crash, without any external intervention.

Another advantage of the invention is the possibility of transferring registered endpoints from one gatekeeper to another.

## 5 References

- [1] " Call Signaling Protocols and Media Stream Pack-  
etization for Packet Based Multimedia Communications  
Systems" , DRAFT ITU-T Recommendation H.225.0,  
10 Version 2



P a t e n t   c l a i m s

1. An arrangement for distributing and dispatching traffic in a network, especially H.323 generated traffic, which arrangement comprises one or more gatekeepers, here designated as so-called external or real gatekeepers, characterized by the introduction of one or more internal and lightweight gatekeepers, where internal means that they are arranged in a certain domain, and they are lightweight in the sense that each gatekeeper support a limited range of the H.323 message set, each such lightweight gatekeeper basically understanding any message used by any endpoint when registering to a real gatekeeper and that each lightweight gatekeeper is adapted to put an endpoint of its domain in contact with an external or real gatekeeper, outside said domain.

2. Arrangement as claimed in claim 1, characterized in that each lightweight gatekeeper is adapted to basically understand a subset of the messages as stated in H.225, i.e. comprising for example GRQ (Gatekeeper Request), GCF (Gatekeeper Confirm), GRJ (Gatekeeper Reject), IRR (Information Request Response), IRQ (Information Request), RAI (Resource Availability Indication), RAC (Resource Availability Confirm), RRQ (Registration Request), RCF (Registration Confirm), RRJ (Registration Reject).

3. Arrangement as claimed in claim 2, characterized in that each real gatekeeper is arranged to register a lightweight gatekeeper during

start-up, and each lightweight gatekeeper is arranged to maintain a list or table of valid real gatekeepers.

4. Arrangement as claimed in claim 3,

5 c h a r a c t e r i z e d i n that said table is supplemented with resource information indicating the load on each particular real gatekeeper.

5. Arrangement as claimed in claim 4,

10 c h a r a c t e r i z e d i n that said table is supplemented with information relating to quality of service and cost.

6. Arrangement as claimed in claim 5,

15 c h a r a c t e r i z e d i n that the proprietary non-StandardData field of GCF and GRJ messages are used for exchanging information between a lightweight gatekeeper and any external real gatekeeper, which field is used to convey information used in said supplementary fields of said table.  
20 ble.

7. Arrangement as claimed in claim 6,

c h a r a c t e r i z e d i n that the proprietary non-StandardData field of the GRQ message is used by the client  
25 to communicate for example the desired cost level, type of QoS, etc., to the real gatekeeper in question.

8. Arrangement as claimed in any claim 6 or 7,

c h a r a c t e r i z e d i n that for example the  
30 first byte of the nonStandardData field in the GCF message may contain an integer indicating the load of the real gatekeeper.

9. Arrangement as claimed in any of the claims 4-8,  
c h a r a c t e r i z e d i n that lightweight gate-  
keeper may update its internal table or tables statically,  
5 i.e. by management, an example of static configuration set-  
ting being that between 0800 and 1000 a certain external  
gatekeeper may exclude handling GRQs coming from any light-  
weight gatekeeper.
- 10 10. Arrangement as claimed in any of the claims 4-8,  
c h a r a c t e r i z e d i n that each lightweight  
gatekeeper is adapted to update its internal table or ta-  
bles partly dynamically, e.g. on GCF, GRJ and RAI received  
from any real gatekeeper.
- 15 11. Arrangement as claimed in any of the claims 4-8,  
c h a r a c t e r i z e d i n that means for exchanging  
such information comprises protocols like TCP, UDP, or such  
as Java/RMI, Corba, etc.
- 20 12. Arrangement as claimed in any of the preceding claims,  
c h a r a c t e r i z e d i n that any lightweight  
gatekeeper is adapted so as to put an endpoint in contact  
with a real gatekeeper according to the following alterna-  
25 tives:
- 1) Forward the GRQ to a randomly picked real gatekeeper
  - 2) Forward the GRQ based on internal information, exam-  
30 ples of such internal information being QoS, load,  
cost, time of day, etc.

- 3) Forward the GRQ to a specific real gatekeeper to a basis of other criterias
- 4) By forward is meant explicitly, i.e. plain forward of the GRQ to an external gatekeeper, or implicitly, i.e. the address of the external gatekeeper is directly provided in the internal gatekeeper's GCF towards the endpoint
- 10 13. Arrangement as claimed in any of the preceding claims, characterized in that one internal light-weight gatekeeper is adapted to communicate with a plurality of endpoints, said plurality of endpoints only knowing about said one internal gatekeeper and thereby avoiding re-
- 15 configuration.

1/4

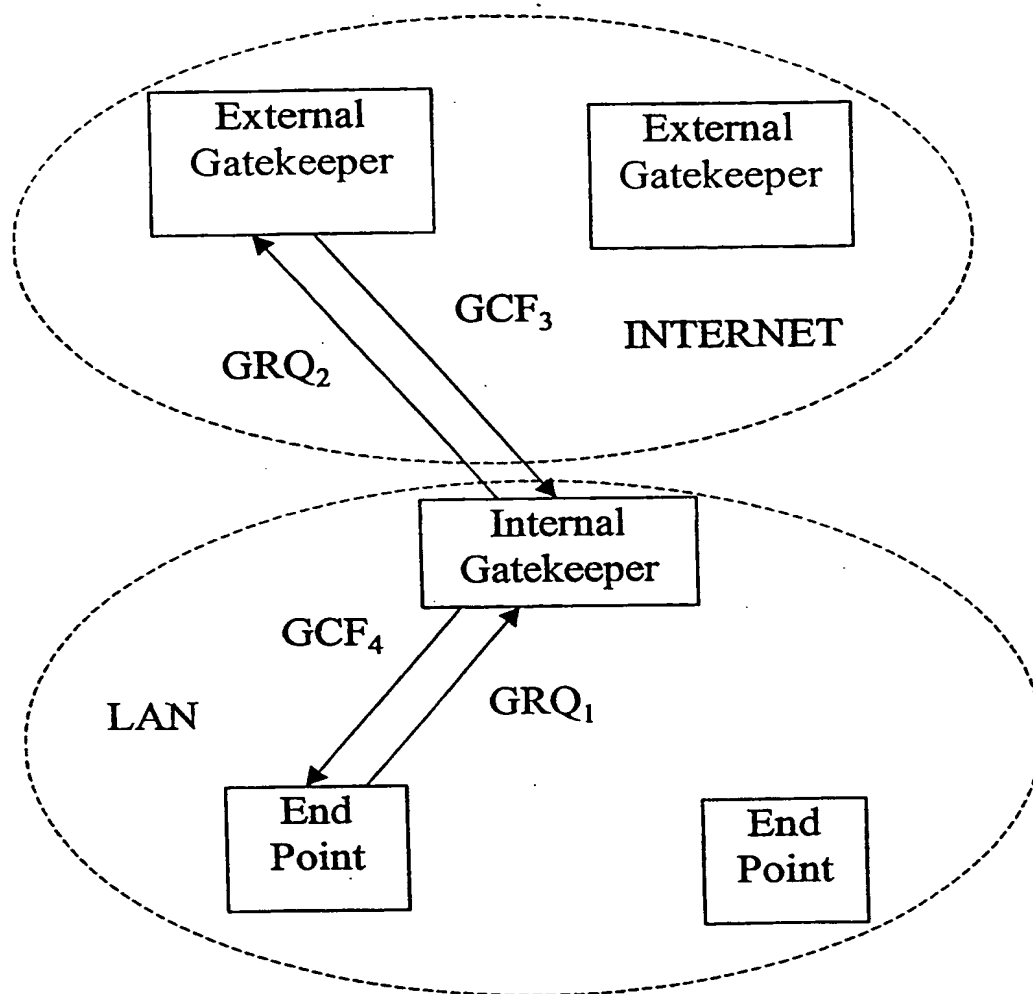


Figure 1

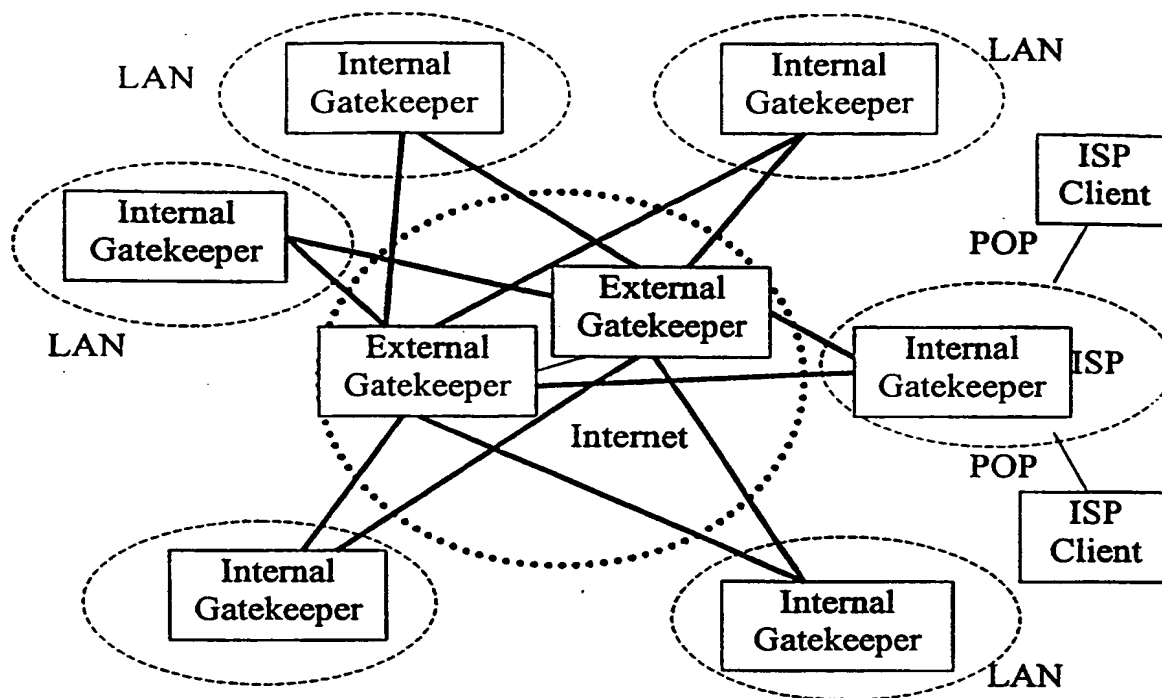


Figure 2

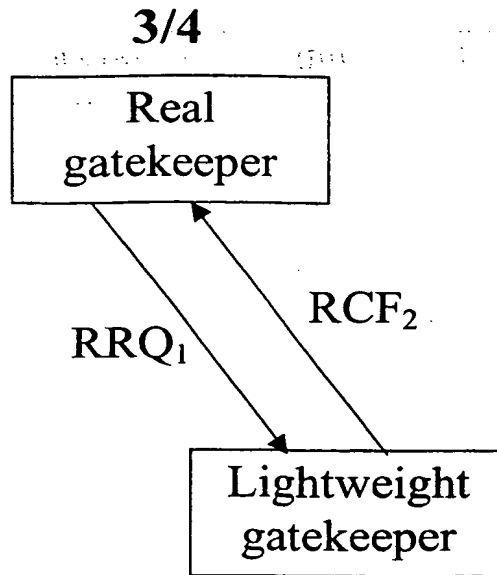


Figure 3: Gatekeeper registration during start-up

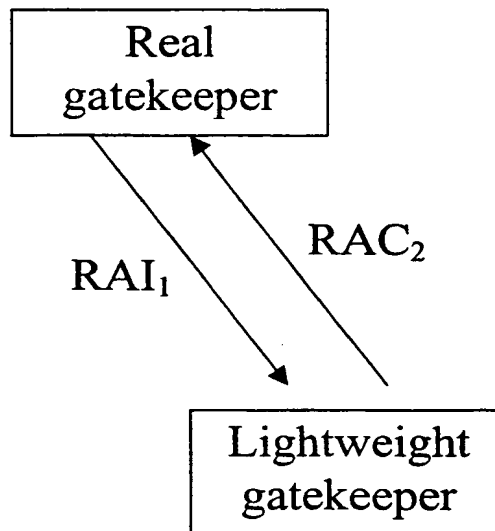


Figure 4: Resource information exchange

4/4

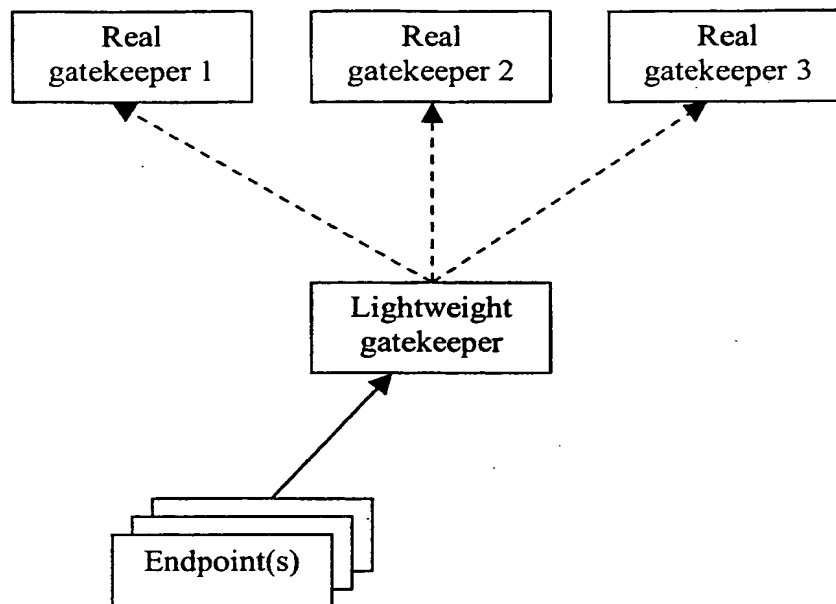


Figure 5: System overview



## INTERNATIONAL SEARCH REPORT

International Application No

PC NO 00/00030

A. CLASSIFICATION OF SUBJECT MATTER  
IPC 7 H04L12/66

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	RADHIKA R. ROY: "Framework for H.323 Inter-Gatekeeper Communications" TELECOMMUNICATION STANDARDIZATION SECTOR APC-1385, 8 - 11 June 1998, pages 1-8, XP002900978 Cannes, FR. page 7	1-13
Y	RADHIKA R. ROY: "Distributed Gatekeeper Architecture for H.323-based Multimedia Telephony" IEEE CONFERENCE ON LOCAL COMPUTER NETWORKS, LCN'99, 1999, pages 73-76, XP002900979 the whole document	1-13
	--- -/--	

☒ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.

## \* Special categories of cited documents :

- \*A\* document defining the general state of the art which is not considered to be of particular relevance
- \*E\* earlier document but published on or after the international filing date
- \*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- \*O\* document referring to an oral disclosure, use, exhibition or other means
- \*P\* document published prior to the international filing date but later than the priority date claimed

- \*T\* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- \*X\* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- \*Y\* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- \*&\* document member of the same patent family

Date of the actual completion of the international search

3 May 2000

Date of mailing of the international search report

20. 06. 2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Mans Marklund/CL

# INTERNATIONAL SEARCH REPORT

International Application No

PC NO 00/00030

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	<p>SENTHIL SENGODAN: "On the Use of Multicast Scope for Gatekeeper Discovery" TELECOMMUNICATION STANDARDIZATION SECTOR APC-1382,  June 1998 (1998-06), pages 1-4,  XP002900980  Cannes, FR.  the whole document</p> <p style="text-align: center;">---</p>	1-13
A	<p>WO 98 17048 A (LANG RUSSELL JOHN ;BRITISH TELECOMM (GB); POTTER JOHN MORGAN MELBO)  23 April 1998 (1998-04-23)  the whole document</p> <p style="text-align: center;">-----</p>	1-13

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PC NO 00/00030

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9817048 A	23-04-1998	AU 4630597 A EP 0932972 A	11-05-1998 04-08-1999
-----			

**THIS PAGE BLANK (USPTO)**